

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-348486

(43)Date of publication of application : 22.12.1994

(51)Int.Cl.

G06F 9/06

G06F 3/06

G06F 9/445

G06F 11/00

(21)Application number : 03-166955

(71)Applicant : ACER INC

(22)Date of filing : 08.07.1991

(72)Inventor : LIN PEI-HU

(30)Priority

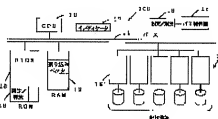
Priority number : 91 689018 Priority date : 22.04.1991 Priority country : US

(54) METHOD AND SYSTEM FOR PROTECTING COMPUTER SYSTEM AGAINST COMPUTER VIRUS

(57)Abstract:

PURPOSE: To protect a computer system from the attack of a computer virus by detecting the virus and preventing its attack in a boot mode.

CONSTITUTION: A set/open switch 16 is set to inhibit the writing operations to a storage 14 before a boot program is loaded and carried out. That is, only the fetching of data of the storage 14 is possible when the switch 16 is set. A computer system 100 can load and carry out the boot program and a basic device after the switch 16 is set. Then the system 100 checks whether its computer is attacked by a virus after theses program and device are carried out. In this case, an interrupt vector loaded in a RAM 12 is compared with its corresponding normal value. The normal value of the interrupt vector which is not infected can be stored in the storage 14.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許公開番号

特開平6-348486

(43) 公開日 平成6年(1994)12月22日

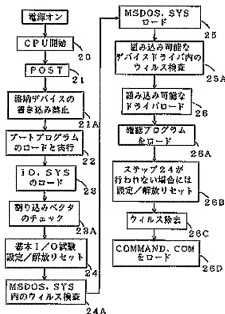
(51) Int. Cl. ⁵	識別記号	片内整理番号	P I	技術表示箇所
G 0 6 F 9/06 3/06 9/445	3 0 4 K	9907-5B 9907-5B	G 0 6 F 9/ 08 4 2 0 S	5 5 0 Z
審査請求 未請求 請求限の数10 O L (全 7 頁) 最終頁に続く				
(21) 出願番号	特願平3-168955	(71) 出願人	591134559	
(22) 出願日	平成3年(1991)7月8日		エイサー・インコーポレイテッド 台湾シン・チュウ・サイエンス・ベイス・ト・ インダストリアル・パーク、シン・アーン・ ロード・?	
(31) 優先権主張番号	689018	(72) 発明者	ベイ・フー・リン	
(32) 優先日	1991年4月22日		台湾タイ・ベイス・アーン、タン・シュイ・ チェン、ベータ・オリ・リー、2-1	
(33) 優先権主張国	米国 (US)	(74) 代理人	弁理士 宮谷 警 (外2名)	

(54) 【発明の名称】 コンピュータウィルスからコンピュータシステムを保護するための方法及びシステム

(57) 【要約】

【目的】 本発明は、ウィルスを検出して、ブート時のウィルスの攻撃を防止することにより、コンピュータウィルスの攻撃からコンピュータシステムを保護するためのシステム及び方法を提供する。

【構成】 本発明によれば、ブート処理前にシステムの格納デバイスの修正を不可能にし、システムの割り込みベクタの健全性を検査することにより、上記目的が達成される。



(2)

特開平6-348486

1

2

【特許請求の範囲】

【請求項1】 ウィルスによる攻撃に対する保護を備えたコンピュータシステムであって：システムにブートプログラムを入力し、データを格納する能力を有する少なくとも1つの格納装置と；ブート時に前記格納装置内のデータにウィルスが影響を与えることを防止するための手段と；かと成ることを特徴とするシステム。

【請求項2】 前記防止手段が、ブートプログラムのロード前に、データの格納を禁止するための手段から成ることを特徴とする、請求項1に記載のシステム。

【請求項3】 前記防止手段が、ブート時にウィルスの存在を検出するための手段から成ることを特徴とする、請求項1に記載のシステム。

【請求項4】 システムが、一組の割り込みベクタに 대응して複数の入力/出力装置と相互作用し、前記検出手段が、前記割り込みベクタが修正されたかどうかを検査するための手段から成ることを特徴とする、請求項3に記載のシステム。

【請求項5】 プログラムの所定の特性を格納するための手段と、前記格納された特性とシステムにロードされる対応プログラムの特性を比較するための手段とを、さらに含むことを特徴とする、請求項1に記載のシステム。

【請求項6】 システム内にブートプログラムを入力しデータ格納する性能を有する少なくとも1つの格納装置を備えたコンピュータシステムをウィルスの攻撃から保護するための方法であって：システムをブートプログラムを実行するステップと；さらにブート時に格納装置内のデータにウィルスが影響を与えないように防止するステップと；から成ることを特徴とする方法。

【請求項7】 前記防止ステップが、前記ブートプログラムのロード前のデータの格納を禁止するためのサブステップから成ることを特徴とする、請求項6に記載の方法。

【請求項8】 前記防止ステップが、ブート時にウィルスの存在を検出するステップから成ることを特徴とする、請求項6に記載の方法。

【請求項9】 前記システムが、一組の割り込みベクタに 대응して複数の入力/出力装置と相互作用し、前記検出手段が前記割り込みベクタが修正されたかどうかを検査するステップから成ることを特徴とする、請求項8に記載の方法。

【請求項10】 さらに、プログラムのものである特性を格納するステップと前記格納されたプログラムの特性と、システムにロードされる対応プログラムの特性とを比較するステップから成ることを特徴とする、請求項9に記載の方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、コンピュータウイルスとして一般に知られている外敵からコンピュータシステ

ムを保護するための装置及び方法に関する。

【0002】

【従来の技術】 世界がさらに一層コンピュータ化されるにつれて、データ処理産業の大きな関心の一つはウイルスによるコンピュータシステムに対する攻撃の可能性である。余り深刻でない場合であっても、コンピュータウイルスによる攻撃があった場合は、組織が通常の動作を回復する前に、データやファイルを復元又は回復する必要がある。もっと深刻な場合には、ウイルスにより破壊されたデータ及びファイルは回復不能であり、組織の動作は永久に遮断される。最も深刻な場合には、組織のデータベースの保管が奪取なしに攻撃されて、組織は正確なデータを用いて動作を継続し、結果として、侵害、損失及び被害を被る。

ウイルス問題は、典型的なコンピュータウイルスが、生物ウイルスと同様に、自己複製能力を有しており、ネットワークの接続を介して感染可能であるために、増大しつつある。ウイルスはそれ自体がアプリケーションプログラム及び/又はシステムプログラムに付着する。さらに、比較的無害なウイルスは、(コンピュータシステム内に常駐している間に変身して)「突然変異」し、破壊的なウイルスになる。

【0003】 ウィルスがコンピュータシステムを攻撃する一つの一般的な方法は、ウイルスがシステムの動作及び1/0装置とやり取り可能なように、システム内の割り込みベクタを変更させることによる。したがって、従来の抗ウイルス方法は、ウイルスによる割り込みベクタの変更の試みを検出可能なように、割り込みベクタと割り込みプログラム指令にフックを設定することである。

【0004】 他の従来の抗ウイルス方法においては、システム内で実行されるプログラムが、最初に、プログラムが変更されたかどうかを検出するために自己診断を行う。プログラムが変更され、それが感染であった場合には、システム内のプログラムの実行が禁止される。

【0005】 他の従来の抗ウイルス方法においては、悪戯しない状態のふるふるの所定の特性(例えば、サブチェック)が格納される。プログラムが実行される前に、これらの特性が再生されて、対応する格納された相手側と比較され、変更されたかどうかが判定される。

【0006】

【発明が解決しようとする課題】 しかし、これらの従来の方法は3つの理由から満足いくものではない。第1に、これらの従来の方法の動作は、コンピュータのオペレーティングシステム(例えば、DOS)の支援を必要とする。オペレーティングシステムは、コンピュータシステムが完全にブートした後にのみ機能可能なので、これらの従来の方法は、コンピュータシステムのブート時、例えば、オペレーティングシステムの組み込み前に攻撃をしかけるウイルスからコンピュータを守ることができない。第2に、従来の方法は、オペレーティングシ

(3)

待間平6-348486

4

システムをバイパスし、ハードウェア。又はBIOS上で直接動作するウィルスを防止することはできない。第3に、乗客の抗ウィルスシステムは、オペレーティングシステムのモジュール(例えば、IO.SYS、MSDOS.SYSやCOMMAND.COM)に常驻するウィルスを防止することができない。

[0007]従って、ウィルスがコンピュータシステムに入ること防止するだけではなく、すでにコンピュータシステムに常驻するウィルスを除去し不能化することにより、コンピュータシステムをウィルスから保護するための装置及び方法に対する必要性が存在する。さらに、また、システムのブートアップ時にウィルスから保護する必要性が存在する。

[0008]

[課題を解決するための手段] ウィルスからコンピュータシステムを保護するための本発明の好適な実施例は、システムのブート前にデータをコンピュータシステムの記憶装置に格納することを禁止するための手段と、すでにシステム内にロードされたプログラムの健全性を検査するための手段と、さらに、検査手段にตอบสนองして、システム内にロードされたプログラムがウィルスに感染していない場合にデータの記憶装置への格納を可能化するための手段と、から構成される。

[0009]さらに、本発明の好適な実施例は、コンピュータシステム内にロードされて実行されるプログラムがウィルスに感染していないことを検出するための手段と、システム内に常驻している可能性のあるウィルスを除去するための手段と、から構成される。

[0010]

[実施例] 図1は、本発明の好適な実施例を含む典型的なコンピュータシステム100のブロック図である。コンピュータシステム100は、バス1を介して、RAM12とROM13と複数のI/O装置などの他の附属装置と相互動作する。これらのI/O装置14は、データ記憶装置(例えば、フロッピーディスクやハードディスク)、キーボード(図示せず)、モニタ(図示せず)などの基本的装置を含んでいる。I/O装置14は、さらに、テープやCD-ROM(図示せず)のような、1又はそれ以上の呼び出し組み合わせ可能な装置(任意選択)を含んでいる。

[0011]記憶装置14の1つは、(電源オンのような)起動時にプログラムをブートするために用いることが可能である。このように用いられるので、このような記憶装置14はブート装置とも呼ばれる。

[0012]ROM13は、コンピュータシステム100のI/O装置14とインタフェース動作を実行するための基本入力システム(BIOS)として一般に知られているソフトウェア指令を含んでいる。さらに、ROM13には、ブート装置からブートプログラムをロードするよう動作するソフトウェアルーチンが格納されてい

る。ブートプログラムは、通常は、コンピュータシステム100の電源オン時、又はシステムの初期化が必要とされる場合に、実行される。

[0013]今日の大部分のコンピュータシステムで行われているように、I/O装置14は割り込みを発生することにより、CPU10と通信を行う。CPUは割当てられた個々の割り込みコードを介してI/O装置の中から割り込みを識別する。CPU10のI/O装置に対する応答は、とりわけ、割り込みを発生する装置14に依存している。割り込みベクタは、異なる割り込み処理ルーチンにCPU10を向けるために設けられる。例えば、今日の多くのパーソナルコンピュータでは、256の割り込みベクタが割当てられている。

[0014]割り込みベクタは、BIOSの実行によるコンピュータシステム100の起動(又はブート)の際に発生される。装置割り込みに対するCPU10の応答は時間を経るごとに変化される必要があるため、割り込みベクタも、CPU10を異なる割り込み処理ルーチンに向けることが可能なように、時間を経るごとに修正する必要がある。割り込みベクタの修正を可能にするために、割り込みベクタはコンピュータシステム100の動作時にRAM12内に格納される。

[0015]効率とユーザとの信頼性を増加させるために、大多数のコンピュータシステムは、典型的にはオペレーティングシステムプログラム(例えば、マイクロソフト社のディスクオペレーティングシステムであるMSDOS)により制御される。オペレーティングシステムは、(IO.SYSのような)基本I/O装置を駆動して、(例えば、MSDOSのような)他のシステム制御モジュールを制御するためのモジュールから構成される。さらに、オペレーティングシステムは、ユーザにより入力された指令を解釈するための(MSDOSのCOMMAND.COMのような)指令インタプリタを含むことが可能である。

[0016]図2には、コンピュータシステム100の電源が入れた後従来の初期起動の様子が示されており(ブロック20)、CPU10は通常は最初に、ROM13内のBIOSの一部として格納された電源オン自己試験(POST)(ブロック21)を実行する。POST内には誤差がない場合には、ブートプログラムがブート装置からコンピュータシステム100(ブロック22)内にロードされる。ブートプログラムが順次実行されると、オペレーティングシステムモジュール(IO.SYS)がロードされる(ブロック23)。このオペレーティングシステムモジュールは、基本I/O装置14のためのソフトウェアドライバである。気温I/O装置14が次いで試験される(ブロック24)。次いで、オペレーティングシステム(MSDOS.SYS)のコア(ブロック25)、組み込み可能な装置に関するソフトウェアドライバ(ブロック26)、及び指令イン

(4)

特開平6-348486

5

タブリタ (COMMAND.COM) がロードされて、次いで実行される。

【0017】上述の手順の完了後に、ブーティング動作が終了したものと判断されて、コンピュータシステムは通常の動作の準備を完了する。それから、1又はそれ以上のアプリケーションプログラムのロード及び実行を含む指令をユーザから受け取ることが可能になる。

【0018】現在のコンピュータウイルスは、通常は、次のように分類可能である。すなわち、(1)ブート時間感染ウイルス、(2)プログラム感染ウイルス及び(3)システム感染ウイルスである。

【0019】ブート時間感染ウイルスは典型的には、ブート時にブートプログラムをウイルスプログラムと置き換えることによりコンピュータシステムに影響を与えて、システムを制御する。どのようにしてウイルスがコンピュータシステムの制御を奪うかについて説明するために、最初に通常のブーティング手順を説明される。

【0020】コンピュータシステム100が、(感染したフロッピーディスクをフロッピーディスク装置に挿入した場合などに)ウイルスで感染されると、ウイルスはブーティング手順の間に1又はそれ以上の(例えば、ディスク記憶割り込みベクタなどに開する)割り込みベクタを変更し、それがウイルスプログラムを指指するようにする。コンピュータシステム100はBIOSの部分としてウイルスプログラムを認識する。こうして、ウイルスプログラムは、ディスクアクセスに関する割り込み処理プロセスの制御を盗むことが可能になる。例えば、ユーザがディスクからデータにアクセスする時に、ウイルスプログラムが自己をディスクに復写可能になる。コンピュータは通常動作しているように見えるが、コンピュータシステム内のディスクはすでに感染している。

【0021】プログラム感染ウイルスは通常はアプリケーションプログラム内に常駐している。それらは、典型的には、割り込みベクタを修正することによりアプリケーションプログラムの実行の間にコンピュータシステムを攻撃して、システムにウイルスプログラムを実行させる。

【0022】システム感染ウイルスは通常は(10.SYSとMSDOS.SYSなどの)オペレーティングシステムプログラム内に常駐している。それらはブーティング手順時にシステムを攻撃する。

【0023】図3は、図2に示したと同様のシステム起動プロセスの流れ図である。しかし、プロセスは改良されて本発明を組み込んでいる。

【0024】最初に、システムのエラーが入れられて、CPUがステップ20で開始する。システムのエラー時には、POST(ブロック21)で誤りなしに実行されると、ブーティングプログラムがブーティング装置からコンピュータシステム100に通常通りロードされる(ブロック22)。

6

【0025】本発明によれば、ブーティングプログラムがロードされて実行される前に(ブロック23)、設定/開放スイッチ16が記憶装置14への書き込みを禁止するべく設定される(ブロック24)。換言すれば、設定/開放スイッチ16の設定により、記憶装置14を読み出し専用14からのデータの取り込み及び可能になる。

【0026】特定の記憶装置へのデータの格納を禁止するための方法は、いくつかの方法で実行可能である。例えば、コンピュータシステム100のバス制御器15はバス11を通過する全てのI/O動作を画面表示するので、設定/開放スイッチ16の設定に応じて、指定されたI/O装置14に対する書き込み動作を拒絶することが可能である。

【0027】代わりに、設定/開放スイッチ16をROM13に格納されたBIOSに常駐させることが可能である。全てのI/O動作はBIOSの実行により行われるので、BIOSは、設定/開放スイッチ16の設定によりBIOSが効果的にある装置への書き込み指令を無視するように、実行可能である。

【0028】さらに、設定/開放スイッチ16の設定は、(揮発性記憶装置と比較して)、不揮発性スイッチ14に対する書き込みのみを禁止すべきである。これらの装置の内容の完全性のみが保持される必要があるからである。

【0029】設定/開放スイッチ16を設定することにより、ウイルスはブート時に記憶装置14内のデータ/プログラムを攻撃することができなくなる。

【0030】流れ図は設定/開放スイッチ16の設定がコンピュータシステム100のブート前に正しいことを示しているが、スイッチ16はシステムのブート前もしくはその時点で、書き込み動作を禁止するべく設定することが可能である点は、当業者であれば理解できよう。例えば、設定/開放システムの電源オン信号により設定可能である。

【0031】設定/開放スイッチ16が設定された後に、コンピュータシステム100は、ブートプログラムと基本デバイスに関するロードと実行を開始可能になる(ブロック22及び23)。

【0032】これらのプログラムがロードされて実行された後に、コンピュータシステム100は、コンピュータがウイルスにより攻撃されたかどうかを検査するであろう(ブロック23A)。これは、RAM12内にすでにロードされた割り込みベクタを対応する通常の(感染していない)値と比較することにより行われる。割り込みベクタの通常の(感染していない)値は記憶装置14内のどれかに格納可能である。

【0033】代わりに、割り込みベクタのデフォルト値は通常はBIOSのアドレス範囲を指しているため、比較は、ベクタ値がかかる好適な範囲内にあるかどうか

(5)

特開平6-348486

7

8

を検査するだけである。

【0034】實用効果の簡略化で、1つだけの又は特定の組の割り込みベクタがチェックされるべきである。例えば、大部分のブート時感染ウィルスはモニタの割り込みベクタを使用するので、本発明の目的のために、かかる割り込みベクタが変更されたかをチェックするだけで十分である場合もある。

【0035】割り込みベクタの組が変更された場合には、コンピュータシステム100は、ブーティングプログラムがウィルスに感染していることをユーザに知らせる信号を発生するよう、適切な救済行動を起こす(ブロック2)。本発明の好適な実施例によれば、ウィルスインディケータ17は不揮発性記憶装置の1つの中に隠されている。システムがブーティングプログラムを発見すると、ウィルスインディケータが、ブーティング装置が感染したことをユーザに報告するように設定される。ウィルスインディケータ17もまた不揮発性記憶装置内に格納される。

【0036】割り込みベクタが汚染されていない場合には、コンピュータシステムの電源オン動作がシステムドライバ(MSDOS、SYS)(ブロック25)及び組み込み可能なデバイスドライバ(ブロック26)をロードして継続される。しかし、好適な実施例においては、このような各プログラムは、ウィルスが常駐していないと判定された後(ブロック24A及び25A)にのみ、ロードされる。

【0037】別の方法として、感染されていない状態のブーティングプログラムのコピーをコンピュータシステム100内の、ROM13又は不揮発性記憶装置14のいずれかに格納することも可能である。このコピーはブーティング前にブーティング装置からのブートプログラムと比較するために用いられる。

【0038】好適な実施例によれば、いくつかのプログラムモジュール(MSDOS、SYS、組み込み可能なデバイスドライバ、及びCOMMAND.COM)はロードされることが必要であるが、これらがロードされる前にこれらのプログラムの安全性をチェックするための手段が設けられているので、設定/開閉スイッチ16又は16'は、RAM12内の割り込みベクタが変更されていない場合には、この時点でリセット可能である。かかる手段が設けられていない場合には、設定/開閉スイッチ16又は16'は、ステップ26Cの電源オンプロセスの終わりに近づくにリセット可能である。

【0039】好適な実施例では、感染されていない状態のシステムモジュール(MSDOS、SYS及び組み込み可能なデバイスドライバ)のそれぞれのチェックサムが格納される。これらのモジュールの各々がロードされて実行される前に、対応するチェックサムが計算されて、格納された値と比較されて、オペレーティングシステムモジュールが感染されたかどうか判定される。比

較により変更がないことが示されると、システムはプログラムをロードして通常の処理を進める。そうでない場合には、警告信号とウィルスインディケータ17が、ユーザにブーティング装置の交換を報告するように設定される。

【0040】電源オン手順は、ここではとんと完了し、CPU10の作動準備が完了する。しかし、システムをファイルタイプ(又は、プログラムタイプ)ウィルスから保護するために、検証プログラムが、プログラムタイプウィルスがコンピュータシステム内に入り込むのを防止するために好適な環境に組み込まれる。(ブロック26A及び26B)。検証プログラムは、ユーザがシステムに感染されていない状態の各アプリケーションプログラムに固有の特性(例えば、チェックサム)を有えることを要求する。

【0041】システムは、ステップ26Bにおいて与えられた特性に対してアプリケーションプログラムの特性をチェックする。特性が整合した場合にはプログラムの実行が許可される。

【0042】本発明の別の好適な実施例によれば、ウィルス除去手段が設けられる。ウィルススクリーニングプログラムは上述のステップで検出されたウィルスを除去する。ウィルス除去手段は、ブーティングプログラム、オペレーティングシステムモジュール及び組み込み可能なデバイスドライバの良好なコピーを格納する。ウィルスが前述のブーティングプロセスで検出されると、プログラムの良好なコピーが不揮発性読み出し専用記憶装置から、前のブーティングプロセスで用いられた不良コピー上に復写される。上述のウィルス除去方法の1つは、検証プログラム及びウィルス除去プログラム内のウィルスの存在を検出するために用いることも可能である。

【0043】

【発明の効果】本発明の保護システムによれば、ブーティング手順の間におけるウィルス保護の不利益を減じることが可能である。保護システムはブーティング手順を制御して、正確にかつ効果的にシステムをコンピュータウィルスの汚染から防止可能である。さらに、保護システムの好適な実施例によれば、プログラムタイプのウィルスによる被害を防止し可能であり、さらに、ウィルス検出手段が設けられる。このような効果は従来の保護システムによって得ることができない。このように、本発明の保護システムによればコンピュータウィルスに起因する損害を大幅に低減可能である。

【0044】もちろん、上述の記載は本発明の好適な実施例に過ぎず、各組の変更及び修正を本発明の真の精神及び広い観点に照らして実施することが可能である。

【図面の簡単な説明】

【図1】本発明が組み込まれるコンピュータシステムのブロック図である。

(6)

特開平6-348486

10

【図2】コンピュータシステムの典型的な電源オン動作の流れ図である。

【図3】本発明のウィルス防止システムの好適な実施例のブロック図である。

【符号の説明】

100 コンピュータシステム

10 CPU

* 11 バス

12 RAM

13 ROM

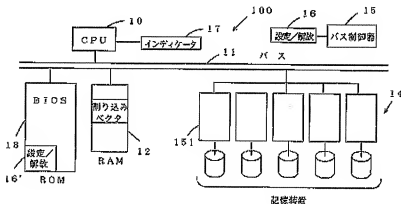
14 I/O装置

15 バス制御器

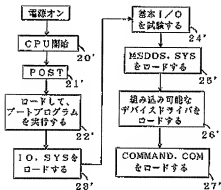
16, 16' 設定/開放スイッチ

* 17 ウィルスインディケーター

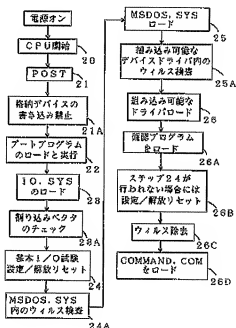
【図1】



【図2】



【図3】



(7)

特開平6-348486

フロントページの続き

(51)Int. Cl.⁷

G 0 6 F 11/00

識別記号

3 5 0 M

序内整圖書号

F I

技術表示箇所